

1 John J. Nelson (SBN 317598)
2 **MILBERG COLEMAN BRYSON**
3 **PHILLIPS GROSSMAN, PLLC**
4 280 S. Beverly Drive
5 Beverly Hills, CA 90212
6 Tel.: (858) 209-6941
7 jnelson@milberg.com

8 *Attorney for Plaintiff and the Proposed Class*

9
10 **UNITED STATES DISTRICT COURT**
11 **FOR THE CENTRAL DISTRICT OF CALIFORNIA**

12 JOSEPH BIONDI, on behalf of himself
13 individually and on behalf of all others
14 similarly situated,

15 Plaintiff,

16 v.

17 MULTI-FINELINE ELECTRONIX,
18 INC.,

19 Defendant.
20

Case No.: _____

CLASS ACTION COMPLAINT

DEMAND FOR A JURY TRIAL

21 Plaintiff Joseph Biondi (“Plaintiff”) brings this Class Action Complaint
22 (“Complaint”) against Defendant Multi-Fineline Electronix, Inc. (“Defendant”) as
23 an individual and on behalf of all others similarly situated, and alleges, upon
24 personal knowledge as to his own actions and his counsels’ investigation, and upon
25 information and belief as to all other matters, as follows:
26
27
28

INTRODUCTION

1
2 1. This class action arises out of the recent cyberattack and data breach
3 (“Data Breach”) that was perpetuated against Defendant, “one of the largest flexible
4 printed circuit manufacturers, assemblers and suppliers[.]”¹
5

6 2. Plaintiff’s and Class Members’ sensitive personal information—which
7 they entrusted to Defendant—was compromised and unlawfully accessed due to the
8 Data Breach.
9

10 3. Defendant collected and maintained certain personally identifiable
11 information of the putative Class Members (defined below), who are (or were)
12 employees and/or employee-beneficiaries at Defendant.
13

14 4. The Private Information compromised in the Data Breach included
15 Plaintiff’s and Class Members’ names, dates of birth, driver’s license numbers or
16 state identification numbers, financial account numbers, financial account access
17 information, passport numbers, payment card numbers, payment card access
18 information, Social Security Numbers, and usernames and passwords (“personally
19 identifying information” or “PII”) and medical and health insurance information,
20 which is protected health information (“PHI”, and collectively with PII, “Private
21 Information”) as defined by the Health Insurance Portability and Accountability Act
22 of 1996 (“HIPAA”).
23
24
25
26

27 ¹ <https://www.mflex.com/about-mflex/>
28

1 5. The Private Information compromised in the Data Breach was targeted
2 and exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals.

3
4 6. As a result of the Data Breach, Plaintiff and Class Members suffered
5 concrete injury in fact including, but not limited to: (i) invasion of privacy; (ii) theft
6 of their Private Information; (iii) lost or diminished value of Private Information;
7 (iv) lost time and opportunity costs associated with attempting to mitigate the actual
8 consequences of the Data Breach; (v) lost opportunity costs associated with
9 attempting to mitigate the actual consequences of the Data Breach; (vi) experiencing
10 an increase in spam calls, texts, and/or emails; (vii) Plaintiff's Private Information
11 being disseminated on the dark web, according to Experian; (viii) statutory damages;
12 (ix) nominal damages; and (x) the continued and certainly increased risk to their
13 Private Information, which: (a) remains unencrypted and available for unauthorized
14 third parties to access and abuse; and (b) remains backed up in Defendant's
15 possession and is subject to further unauthorized disclosures so long as Defendant
16 fails to undertake appropriate and adequate measures to protect the Private
17 Information.
18
19
20
21

22 7. The Data Breach was a direct result of Defendant's failure to implement
23 adequate and reasonable cyber-security procedures and protocols necessary to
24 protect its employees' and beneficiaries' Private Information from a foreseeable and
25 preventable cyber-attack.
26
27
28

1 8. Plaintiff brings this class action lawsuit on behalf of those similarly
2 situated to address Defendant's inadequate safeguarding of Class Members' Private
3 Information that it collected and maintained, and for failing to provide timely and
4 adequate notice to Plaintiff and other Class Members that their information had been
5 subject to the unauthorized access by an unknown third party and precisely what
6 specific type of information was accessed.
7

8
9 9. Defendant maintained the Private Information in a reckless manner. In
10 particular, the Private Information was maintained on Defendant's computer
11 network in a condition vulnerable to cyberattacks. Upon information and belief, the
12 mechanism of the cyberattack and potential for improper disclosure of Plaintiff's
13 and Class Members' Private Information was a known risk to Defendant, and thus,
14 Defendant was on notice that failing to take steps necessary to secure the Private
15 Information from those risks left that property in a dangerous condition.
16
17

18 10. Defendant disregarded the rights of Plaintiff and Class Members by,
19 *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate
20 and reasonable measures to ensure its data systems were protected against
21 unauthorized intrusions; failing to disclose that they did not have adequately robust
22 computer systems and security practices to safeguard Class Members' Private
23 Information; failing to take standard and reasonably available steps to prevent the
24
25
26
27
28

1 Data Breach; and failing to provide Plaintiff and Class Members prompt and
2 accurate notice of the Data Breach.

3
4 11. Plaintiff's and Class Members' identities are now at risk because of
5 Defendant's negligent conduct because the Private Information that Defendant
6 collected and maintained is now in the hands of data thieves.

7
8 12. Armed with the Private Information accessed in the Data Breach, data
9 thieves have already engaged in identity theft and fraud (including the fraud suffered
10 by Plaintiff described below), and can in the future commit a variety of crimes
11 including, *e.g.*, opening new financial accounts in Class Members' names, taking out
12 loans in Class Members' names, using Class Members' information to obtain
13 government benefits, filing fraudulent tax returns using Class Members'
14 information, obtaining driver's licenses in Class Members' names but with another
15 person's photograph, and giving false information to police during an arrest.

16
17 13. As a result of the Data Breach, Plaintiff and Class Members have been
18 exposed to a present and continuing risk of fraud and identity theft. Plaintiff and
19 Class Members must now and in the future closely monitor their financial accounts
20 to guard against identity theft.

21
22 14. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*,
23 purchasing credit monitoring services, credit freezes, credit reports, or other
24 protective measures to deter and detect identity theft.

1 This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a)
2 because all claims alleged herein form part of the same case or controversy.
3

4 21. This Court has personal jurisdiction over Defendant because it operates
5 and maintains its principal place of business in this District and the computer
6 systems implicated in this Data Breach are likely based in this District. Further,
7 Defendant is authorized to and regularly conducts business in this District and makes
8 decisions regarding corporate governance and management of its businesses in this
9 District, including decisions regarding the security measures to protect its
10 employees' Private Information.
11
12

13 22. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d)
14 because a substantial part of the events giving rise to this action occurred in this
15 District, including decisions made by Defendant's governance and management
16 personnel or inaction by those individuals that led to the Data Breach; Defendant's
17 principal place of business is located in this district; Defendant maintains Class
18 Members' Private Information in this District; and Defendant caused harm to Class
19 Members residing in this District.
20
21

22 **FACTUAL ALLEGATIONS**

23 ***Defendant's Business***

24
25
26
27
28

1 23. Defendant is “one of the largest flexible printed circuit manufacturers,
2 assemblers and suppliers[.]”²

3
4 24. Class Members are current or former employees and/or employee
5 beneficiaries at Defendant.

6 25. As a condition of obtaining employment and/or obtaining certain
7 employee benefits at Defendant, Defendant requires that its employees and
8 employee beneficiaries, including Class Members, entrust it with highly sensitive
9 personal information.
10

11
12 26. The information held by Defendant in its computer systems at the time
13 of the Data Breach included the unencrypted Private Information of Plaintiff and
14 Class Members.
15

16 27. Upon information and belief, Defendant made promises and
17 representations to its employees and employee beneficiaries, including Class
18 Members, that the Private Information collected from them as a condition of their
19 employment and/or receiving benefits at Defendant would be kept safe, confidential,
20 that the privacy of that information would be maintained, and that Defendant would
21 delete any sensitive information after it was no longer required to maintain it.
22
23

24 28. Plaintiff and Class Members provided their Private Information to
25 Defendant with the reasonable expectation and on the mutual understanding that
26

27 ² <https://www.mflex.com/about-mflex/>
28

1 Defendant would comply with its obligations to keep such information confidential
2 and secure from unauthorized access.

3
4 29. Plaintiff and Class Members have taken reasonable steps to maintain
5 the confidentiality of their Private Information. Plaintiff and Class Members relied
6 on the sophistication of Defendant to keep their Private Information confidential and
7 securely maintained, to use this information for necessary purposes only, and to
8 make only authorized disclosures of this information. Plaintiff and Class Members
9 value the confidentiality of their Private Information and demand security to
10 safeguard their Private Information.
11
12

13 30. Defendant had a duty to adopt reasonable measures to protect the
14 Private Information of Plaintiff and Class Members from involuntary disclosure to
15 third parties. Defendant has a legal duty to keep employees' Private Information safe
16 and confidential.
17

18 31. Defendant had obligations created by FTC Act, contract, industry
19 standards, and representations made to Plaintiff and Class Members, to keep their
20 Private Information confidential and to protect it from unauthorized access and
21 disclosure.
22
23

24 32. Defendant derived a substantial economic benefit from collecting
25 Plaintiff's and Class Members' Private Information. Without the required
26
27
28

1 submission of Private Information, Defendant could not perform the services it
2 provides.

3
4 33. By obtaining, collecting, using, and deriving a benefit from Plaintiff's
5 and Class Members' Private Information, Defendant assumed legal and equitable
6 duties and knew or should have known that it was responsible for protecting
7 Plaintiff's and Class Members' Private Information from disclosure.
8

9 ***The Data Breach***

10 34. On or about February 8, 2024, Defendant, began sending Plaintiff and
11 other Data Breach victims a Notice of Data Security Incident letter (the "Notice
12 Letter"), informing them that:
13

14 On or about January 31, 2024, Multi-Fineline Electronix, Inc. ("MFLEX")
15 learned that a network compromise by an unauthorized party may have
16 resulted in the exposure of your personal information. It appears the
17 compromise began on approximately December 1, 2022, and ended on
18 approximately January 2, 2023.

19 . . .

20 The personal information affected by the exposure may have included your:
21 first and last name, date of birth, driver's license number or state identification
22 number, financial account number, financial account access information,
23 health insurance identification number, information related to medical
24 treatment or diagnosis, passport number, payment card number, payment card
25 access information, Social Security Number, and/or username and password.³
26

27 ³ The "Notice Letter". A sample copy is available at
28 <https://oag.ca.gov/ecrime/databreach/reports/sb24-580693>

1 35. Omitted from the Notice Letter were the details of the root cause of the
2 Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to
3 ensure such a breach does not occur again. To date, these critical facts have not been
4 explained or clarified to Plaintiff and Class Members, who retain a vested interest in
5 ensuring that their Private Information remains protected.
6

7
8 36. This “disclosure” amounts to no real disclosure at all, as it fails to
9 inform, with any degree of specificity, Plaintiff and Class Members of the Data
10 Breach’s critical facts. Without these details, Plaintiff’s and Class Members’ ability
11 to mitigate the harms resulting from the Data Breach is severely diminished.
12

13 37. Defendant did not use reasonable security procedures and practices
14 appropriate to the nature of the sensitive information they were maintaining for
15 Plaintiff and Class Members, causing the exposure of Private Information, such as
16 encrypting the information or deleting it when it is no longer needed.
17

18 38. The attacker accessed and acquired files Defendant shared with a third
19 party containing unencrypted Private Information of Plaintiff and Class Members,
20 including their Social Security numbers, PHI, and other sensitive information.
21 Plaintiff’s and Class Members’ Private Information was accessed and stolen in the
22 Data Breach.
23
24

25 39. Plaintiff has been informed by Experian that his Private Information
26 has been disseminated on the dark web, and Plaintiff further believes that the Private
27
28

1 Information of Class Members was subsequently sold on the dark web following the
2 Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-
3 attacks of this type.
4

5 ***Data Breaches Are Preventable***

6 40. Defendant did not use reasonable security procedures and practices
7 appropriate to the nature of the sensitive information it was maintaining for
8 Plaintiff and Class Members, causing the exposure of Private Information, such
9 as encrypting the information or deleting it when it is no longer needed.
10

11 41. As explained by the Federal Bureau of Investigation, “[p]revention
12 is the most effective defense against ransomware and it is critical to take
13 precautions for protection.”⁴
14

15 42. To prevent and detect cyber-attacks and/or ransomware attacks
16 Defendant could and should have implemented, as recommended by the United
17 States Government, the following measures:
18

- 19
- 20 • Implement an awareness and training program. Because end users are
21 targets, employees and individuals should be aware of the threat of
22 ransomware and how it is delivered.
 - 23 • Enable strong spam filters to prevent phishing emails from reaching the
24 end users and authenticate inbound email using technologies like Sender
25 Policy Framework (SPF), Domain Message Authentication Reporting and
26

27 ⁴ How to Protect Your Networks from RANSOMWARE, at 3, *available at*:
28 <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>

1 Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to
2 prevent email spoofing.

- 3 • Scan all incoming and outgoing emails to detect threats and filter
4 executable files from reaching end users.
- 5 • Configure firewalls to block access to known malicious IP addresses.
- 6 • Patch operating systems, software, and firmware on devices. Consider
7 using a centralized patch management system.
- 8 • Set anti-virus and anti-malware programs to conduct regular scans
9 automatically.
- 10 • Manage the use of privileged accounts based on the principle of least
11 privilege: no users should be assigned administrative access unless
12 absolutely needed; and those with a need for administrator accounts should
only use them when necessary.
- 13 • Configure access controls—including file, directory, and network share
14 permissions—with least privilege in mind. If a user only needs to read
15 specific files, the user should not have write access to those files,
directories, or shares.
- 16 • Disable macro scripts from office files transmitted via email. Consider
17 using Office Viewer software to open Microsoft Office files transmitted
18 via email instead of full office suite applications.
- 19 • Implement Software Restriction Policies (SRP) or other controls to prevent
20 programs from executing from common ransomware locations, such as
21 temporary folders supporting popular Internet browsers or
22 compression/decompression programs, including the
AppData/LocalAppData folder.
- 23 • Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- 24 • Use application whitelisting, which only allows systems to execute
25 programs known and permitted by security policy.
- 26 • Execute operating system environments or specific programs in a
27 virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.⁵

43. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

⁵ *Id.* at 3-4.

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].⁶

44. Given that Defendant was storing the Private Information of its current and former employees and employee beneficiaries, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

45. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of, upon information and belief, thousands to tens of thousands of current and former individuals, including Plaintiff and Class Members.

Defendant Acquires, Collects & Stores Plaintiff's and Class Members' Private Information

46. Defendant acquires, collects, and stores a massive amount of Private Information on its employees, former employees, employee beneficiaries, and other personnel.

⁶ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>

1 47. As a condition of employment, or as a condition of receiving certain
2 benefits, Defendant requires that employees, former employees, and other personnel
3 entrust it with highly sensitive personal information.
4

5 48. By obtaining, collecting, and using Plaintiff's and Class Members'
6 Private Information, Defendant assumed legal and equitable duties and knew or
7 should have known that it was responsible for protecting Plaintiff's and Class
8 Members' Private Information from disclosure.
9

10 49. Plaintiff and the Class Members have taken reasonable steps to
11 maintain the confidentiality of their Private Information.
12

13 50. Plaintiff and the Class Members relied on Defendant to keep their
14 Private Information confidential and securely maintained, to use this information for
15 business purposes only, and to make only authorized disclosures of this information.
16

17 51. Defendant could have prevented this Data Breach by properly
18 securing and encrypting the files and file servers containing the Private
19 Information of Plaintiff and Class Members.
20

21 52. Upon information and belief, Defendant made promises to Plaintiff
22 and Class Members to maintain and protect their Private Information,
23 demonstrating an understanding of the importance of securing Private
24 Information.
25
26
27
28

1 53. Defendant's negligence in safeguarding the Private Information of
2 Plaintiff and Class Members is exacerbated by the repeated warnings and alerts
3 directed to protecting and securing sensitive data.
4

5 ***Defendant Knew or Should Have Known of the Risk of the Risk Because***
6 ***Employers in Possession of Private Information are Particularly***
7 ***Suspectable to Cyber Attacks***

8 54. Defendant knew and understood unprotected or exposed Private
9 Information in the custody of employers, like Defendant, is valuable and highly
10 sought after by nefarious third parties seeking to illegally monetize that Private
11 Information through unauthorized access.
12

13 55. Data breaches, including those perpetrated against employers that
14 store Private Information in their systems, have become widespread.
15

16 56. In the third quarter of the 2023 fiscal year alone, 7333 organizations
17 experienced data breaches, resulting in 66,658,764 individuals' personal
18 information being compromised.⁷
19

20 57. In light of recent high profile data breaches at other industry leading
21 companies, including, Microsoft (250 million records, December 2019), Wattpad
22 (268 million records, June 2020), Facebook (267 million users, April 2020), Estee
23 Lauder (440 million records, January 2020), Whisper (900 million records, March
24 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant
25
26

27 ⁷ See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/>
28

1 knew or should have known that the Private Information that they collected and
2 maintained would be targeted by cybercriminals.

3
4 58. Indeed, cyber-attacks, such as the one experienced by Defendant,
5 have become so notorious that the Federal Bureau of Investigation (“FBI”) and
6 U.S. Secret Service have issued a warning to potential targets so they are aware
7 of, and prepared for, a potential attack. As one report explained, smaller entities
8 that store Private Information are “attractive to ransomware criminals...because
9 they often have lesser IT defenses and a high incentive to regain access to their
10 data quickly.”⁸

11
12
13 59. At all relevant times, Defendant knew, or reasonably should have
14 known, of the importance of safeguarding the Private Information of Plaintiff and
15 Class Members and of the foreseeable consequences that would occur if
16 Defendant’s data security system was breached, including, specifically, the
17 significant costs that would be imposed on Plaintiff and Class Members as a result
18 of a breach.

19
20
21 60. Plaintiff and Class Members now face years of constant surveillance
22 of their financial and personal records, monitoring, and loss of rights. The Class
23

24
25
26 ⁸ https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection
27
28

1 is incurring and will continue to incur such damages in addition to any fraudulent
2 use of their Private Information.

3
4 61. In the Notice Letter, Defendant makes an offer of 12 months of
5 identity monitoring services. This is wholly inadequate to compensate Plaintiff
6 and Class Members as it fails to provide for the fact victims of data breaches and
7 other unauthorized disclosures commonly face multiple years of ongoing identity
8 theft, financial fraud, and it entirely fails to provide sufficient compensation for
9 the unauthorized release and disclosure of Plaintiff's and Class Members' Private
10 Information.
11
12

13 62. Defendant's offer of credit and identity monitoring establishes that
14 Plaintiff's and Class Members' sensitive Private Information *was* in fact affected,
15 accessed, compromised, and exfiltrated from Defendant's computer systems.
16

17 63. The injuries to Plaintiff and Class Members were directly and
18 proximately caused by Defendant's failure to implement or maintain adequate
19 data security measures for the Private Information of Plaintiff and Class
20 Members.
21

22 64. The ramifications of Defendant's failure to keep secure the Private
23 Information of Plaintiff and Class Members are long lasting and severe. Once
24 Private Information is stolen, particularly Social Security numbers and PHI,
25 fraudulent use of that information and damage to victims may continue for years.
26
27
28

1 65. As a business in custody of current and former employees' and
2 employee beneficiaries' Private Information, Defendant knew, or should have
3 known, the importance of safeguarding Private Information entrusted to them by
4 Plaintiff and Class Members, and of the foreseeable consequences if its data
5 security systems were breached. This includes the significant costs imposed on
6 Plaintiff and Class Members as a result of a breach. Defendant failed, however,
7 to take adequate cybersecurity measures to prevent the Data Breach.
8

9
10 ***Value of PII and PHI***
11

12 66. The Federal Trade Commission ("FTC") defines identity theft as "a
13 fraud committed or attempted using the identifying information of another person
14 without authority."⁹ The FTC describes "identifying information" as "any name
15 or number that may be used, alone or in conjunction with any other information,
16 to identify a specific person," including, among other things, "[n]ame, Social
17 Security number, date of birth, official State or government issued driver's license
18 or identification number, alien registration number, government passport number,
19 employer or taxpayer identification number."¹⁰
20
21
22
23
24
25

26
27 ⁹ 17 C.F.R. § 248.201 (2013).

28 ¹⁰ *Id.*

1 67. The PII of individuals remains of high value to criminals, as
2 evidenced by the prices they will pay through the dark web. Numerous sources
3 cite dark web pricing for stolen identity credentials.¹¹
4

5 68. For example, Personal Information can be sold at a price ranging
6 from \$40 to \$200, and bank details have a price range of \$50 to \$200.¹²
7

8 69. Criminals can also purchase access to entire company data breaches
9 from \$900 to \$4,500.¹³
10

11 70. Social Security numbers, which were compromised for some of the
12 Class Members as alleged herein, for example, are among the worst kind of
13 Private Information to have stolen because they may be put to a variety of
14 fraudulent uses and are difficult for an individual to change. The Social Security
15 Administration stresses that the loss of an individual's Social Security number,
16 as is the case here, can lead to identity theft and extensive financial fraud:
17

18 A dishonest person who has your Social Security number can use it to
19 get other personal information about you. Identity thieves can use your
20 number and your good credit to apply for more credit in your name.
21 Then, they use the credit cards and don't pay the bills, it damages your
22 credit. You may not find out that someone is using your number until

23 ¹¹ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct.
24 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>

25 ¹² *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6,
26 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>

27 ¹³ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>
28

1 you're turned down for credit, or you begin to get calls from unknown
2 creditors demanding payment for items you never bought. Someone
3 illegally using your Social Security number and assuming your identity
4 can cause a lot of problems.¹⁴

5 71. What's more, it is no easy task to change or cancel a stolen Social
6 Security number. An individual cannot obtain a new Social Security number
7 without significant paperwork and evidence of actual misuse. In other words,
8 preventive action to defend against the possibility of misuse of a Social Security
9 number is not permitted; an individual must show evidence of actual, ongoing
10 fraud activity to obtain a new number.

11 72. Even then, a new Social Security number may not be effective.
12 According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit
13 bureaus and banks are able to link the new number very quickly to the old number,
14 so all of that old bad information is quickly inherited into the new Social Security
15 number."¹⁵
16
17
18
19
20
21
22
23
24

25 ¹⁴ Social Security Administration, *Identity Theft and Your Social Security Number*, available at:
26 <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Oct. 17, 2022).

27 ¹⁵ Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR
28 (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft>

1 73. Driver's license numbers, which were compromised in the Data
2 Breach, are incredibly valuable. "Hackers harvest license numbers because they're
3 a very valuable piece of information."¹⁶
4

5 74. A driver's license can be a critical part of a fraudulent, synthetic identity
6 – which go for about \$1200 on the Dark Web. On its own, a forged license can sell
7 for around \$200."¹⁷
8

9 75. According to national credit bureau Experian:

10 A driver's license is an identity thief's paradise. With that one card, someone
11 knows your birthdate, address, and even your height, eye color, and
12 signature. If someone gets your driver's license number, it is also concerning
13 because it's connected to your vehicle registration and insurance policies, as
14 well as records on file with the Department of Motor Vehicles, place of
15 employment (that keep a copy of your driver's license on file), doctor's
16 office, government agencies, and other entities. Having access to that one
17 number can provide an identity thief with several pieces of information they
18 want to know about you. Next to your Social Security number, your driver's
19 license number is one of the most important pieces of information to keep
20 safe from thieves.
21

22 76. According to cybersecurity specialty publication CPO Magazine, "[t]o
23 those unfamiliar with the world of fraud, driver's license numbers might seem like
24
25
26
27
28

¹⁶ *Hackers Stole Customers' License Numbers From Geico In Months-Long Breach*, Forbes, Apr. 20, 2021, available at: <https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658> (last visited July 31, 2023).

¹⁷ <https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658> (last visited on Feb. 21, 2023).

1 a relatively harmless piece of information to lose if it happens in isolation.”¹⁸

2 However, this is not the case. As cybersecurity experts point out:

3
4 “It’s a gold mine for hackers. With a driver’s license number, bad actors can
5 manufacture fake IDs, slotting in the number for any form that requires ID
6 verification, or use the information to craft curated social engineering
7 phishing attacks.”¹⁹

8 77. Victims of driver’s license number theft also often suffer
9 unemployment benefit fraud, as described in a recent New York Times article.²⁰

10 78. Theft of PHI is also gravely serious: “[a] thief may use your name or
11 health insurance numbers to see a doctor, get prescription drugs, file claims with
12 your insurance provider, or get other care. If the thief’s health information is mixed
13 with yours, your treatment, insurance and payment records, and credit report may be
14 affected.”²¹

15
16 79. The greater efficiency of electronic health records brings the risk of
17 privacy breaches. These electronic health records contain a lot of sensitive
18 information (e.g., patient data, patient diagnosis, lab results, medications,
19
20
21

22 ¹⁸ [https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-](https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/)
23 [numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/](https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/) (last visited on
24 Feb. 21, 2023).

25 ¹⁹ *Id.*

26 ²⁰ *How Identity Thieves Took My Wife for a Ride*, NY Times, April 27, 2021, available at:
27 <https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html> (last visited
28 on Feb. 21, 2023).

29 ²¹ *Medical I.D. Theft, EFraudPrevention*
30 [https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20yo-](https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected.)
31 [ur,credit%20report%20may%20be%20affected.](https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected.) (last visited Nov. 6, 2023).

1 prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's
2 complete record can be sold for hundreds of dollars on the dark web. As such,
3 PHI/PII is a valuable commodity for which a "cyber black market" exists where
4 criminals openly post stolen payment card numbers, Social Security numbers, and
5 other personal information on several underground internet websites.
6 Unsurprisingly, the pharmaceutical industry is at high risk and is acutely affected by
7 cyberattacks, like the Data Breach here.

8
9
10 80. Between 2005 and 2019, at least 249 million people were affected by
11 healthcare data breaches.²² Indeed, during 2019 alone, over 41 million healthcare
12 records were exposed, stolen, or unlawfully disclosed in 505 data breaches.²³ In
13 short, these sorts of data breaches are increasingly common, especially among
14 healthcare systems, which account for 30.03 percent of overall health data breaches,
15 according to cybersecurity firm Tenable.²⁴

16
17
18 81. According to account monitoring company LogDog, medical data sells
19 for \$50 and up on the Dark Web.²⁵

20
21
22 ²² <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/> (last
23 accessed July 24, 2023).

24 ²³ <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/> (last accessed
25 July 24, 2023).

26 ²⁴ [https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-
27 incovid-19-era-breaches/](https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/) (last accessed July 24, 2023).

28 ²⁵ Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security
(Oct. 3, 2019), [https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-
sometimes-crush-hospitals/#content](https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content) (last accessed July 20, 2021)

1 82. “Medical identity theft is a growing and dangerous crime that leaves its
2 victims with little to no recourse for recovery,” reported Pam Dixon, executive
3 director of World Privacy Forum. “Victims often experience financial repercussions
4 and worse yet, they frequently discover erroneous information has been added to
5 their personal medical files due to the thief’s activities.”²⁶
6

7
8 83. A study by Experian found that the average cost of medical identity
9 theft is “about \$20,000” per incident and that most victims of medical identity theft
10 were forced to pay out-of-pocket costs for healthcare they did not receive to restore
11 coverage.²⁷ Almost half of medical identity theft victims lose their healthcare
12 coverage as a result of the incident, while nearly one-third of medical identity theft
13 victims saw their insurance premiums rise, and 40 percent were never able to resolve
14 their identity theft at all.²⁸
15
16

17 84. Based on the foregoing, the information compromised in the Data
18 Breach is significantly more valuable than the loss of, for example, credit card
19 information in a retailer data breach because, there, victims can cancel or close
20
21
22

23 ²⁶ Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser Health News, Feb.
24 7, 2014, <https://khn.org/news/rise-of-identity-theft/> (last accessed July 24, 2023).

25 ²⁷ See Elinor Mills, “Study: Medical Identity Theft is Costly for Victims,” CNET (Mar, 3, 2010),
26 <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last accessed July
27 24, 2023).

28 ²⁸ *Id.*; see also *Healthcare Data Breach: What to Know About them and What to Do After One*,
EXPERIAN, [https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-
toknow-about-them-and-what-to-do-after-one/](https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/) (last accessed July 24, 2023).

1 credit and debit card accounts. The information compromised in this Data Breach
2 is impossible to “close” and difficult, if not impossible, to change—Social
3 Security numbers, PHI, dates of birth, and names.
4

5 85. This data demands a much higher price on the black market. Martin
6 Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to
7 credit card information, personally identifiable information and Social Security
8 numbers are worth more than 10x on the black market.”²⁹
9

10 86. Among other forms of fraud, identity thieves may obtain driver’s
11 licenses, government benefits, medical services, and housing or even give false
12 information to police.
13

14 87. The fraudulent activity resulting from the Data Breach may not come
15 to light for years. There may be a time lag between when harm occurs versus
16 when it is discovered, and also between when Private Information is stolen and
17 when it is used. According to the U.S. Government Accountability Office
18 (“GAO”), which conducted a study regarding data breaches:
19
20

21 [L]aw enforcement officials told us that in some cases, stolen data may
22 be held for up to a year or more before being used to commit identity
23 theft. Further, once stolen data have been sold or posted on the Web,
24 fraudulent use of that information may continue for years. As a result,
25

26 ²⁹ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card*
27 *Numbers*, IT World, (Feb. 6, 2015), available at:
28 <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>

1 studies that attempt to measure the harm resulting from data breaches
2 cannot necessarily rule out all future harm.³⁰

3 ***Defendant Fails to Comply with FTC Guidelines***

4 88. The Federal Trade Commission (“FTC”) has promulgated numerous
5 guides for businesses which highlight the importance of implementing reasonable
6 data security practices. According to the FTC, the need for data security should
7 be factored into all business decision-making.
8

9
10 89. In 2016, the FTC updated its publication, Protecting Personal
11 Information: A Guide for Business, which established cyber-security guidelines
12 for businesses. These guidelines note that businesses should protect the personal
13 employee and employee beneficiary information that they keep; properly dispose
14 of personal information that is no longer needed; encrypt information stored on
15 computer networks; understand their network’s vulnerabilities; and implement
16 policies to correct any security problems.³¹
17

18
19 90. The guidelines also recommend that businesses use an intrusion
20 detection system to expose a breach as soon as it occurs; monitor all incoming
21 traffic for activity indicating someone is attempting to hack the system; watch for
22
23

24
25 ³⁰ Report to Congressional Requesters, GAO, at 29 (June 2007), available at:
<https://www.gao.gov/assets/gao-07-737.pdf>

26 ³¹ Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016).
27 Available at [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)
28 [personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)

1 large amounts of data being transmitted from the system; and have a response
2 plan ready in the event of a breach.³²

3
4 91. The FTC further recommends that companies not maintain Private
5 Information longer than is needed for authorization of a transaction; limit access
6 to sensitive data; require complex passwords to be used on networks; use
7 industry-tested methods for security; monitor for suspicious activity on the
8 network; and verify that third-party service providers have implemented
9 reasonable security measures.
10

11
12 92. The FTC has brought enforcement actions against employers for
13 failing to protect employee data adequately and reasonably, treating the failure to
14 employ reasonable and appropriate measures to protect against unauthorized
15 access to confidential consumer data as an unfair act or practice prohibited by
16 Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders
17 resulting from these actions further clarify the measures businesses must take to
18 meet their data security obligations.
19
20

21 93. These FTC enforcement actions include actions against employers
22 over the compromised Private Information of its employees and employee
23 beneficiaries, like Defendant here.
24

25 94. Defendant failed to properly implement basic data security practices.
26

27 ³² *Id.*
28

1 95. Defendant's failure to employ reasonable and appropriate measures
2 to protect against unauthorized access to employees' and employee beneficiaries'
3 Private Information constitutes an unfair act or practice prohibited by Section 5
4 of the FTC Act, 15 U.S.C. § 45.
5

6 96. Upon information and belief, Defendant was at all times fully aware
7 of its obligation to protect the Private Information of its employees and employee
8 beneficiaries. Defendant was also aware of the significant repercussions that
9 would result from its failure to do so.
10

11 ***Defendant Fails to Comply with Industry Standards***
12

13 97. As noted above, experts studying cyber security routinely identify
14 entities in possession of Private Information as being particularly vulnerable to
15 cyberattacks because of the value of the Private Information which they collect
16 and maintain.
17

18 98. Several best practices have been identified that a minimum should be
19 implemented by employers in possession of Private Information, like Defendant,
20 including but not limited to: educating all employees; strong passwords; multi-
21 layer security, including firewalls, anti-virus, and anti-malware software;
22 encryption, making data unreadable without a key; multi-factor authentication;
23 backup data and limiting which employees can access sensitive data. Defendant
24
25
26
27
28

1 failed to follow these industry best practices, including a failure to implement
2 multi-factor authentication.

3
4 99. Other best cybersecurity practices that are standard for employers
5 include installing appropriate malware detection software; monitoring and
6 limiting the network ports; protecting web browsers and email management
7 systems; setting up network systems such as firewalls, switches and routers;
8 monitoring and protection of physical security systems; protection against any
9 possible communication system; training staff regarding critical points.
10 Defendant failed to follow these cybersecurity best practices, including failure to
11 train staff.
12
13

14 100. Defendant failed to meet the minimum standards of any of the
15 following frameworks: the NIST Cybersecurity Framework Version 1.1
16 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6,
17 PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-
18 4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's
19 Critical Security Controls (CIS CSC), which are all established standards in
20 reasonable cybersecurity readiness.
21
22
23

24 101. These foregoing frameworks are existing and applicable industry
25 standards for an employer's obligations to its employees and employee
26 beneficiaries with respect to safeguarding their Private Information. Upon
27
28

1 information and belief, Defendant failed to comply with at least one—or all—of
2 these accepted standards, thereby opening the door to the threat actor and causing
3 the Data Breach.
4

5 ***Common Injuries and Damages***

6 102. As a result of Defendant's ineffective and inadequate data security
7 practices, the Data Breach, and the foreseeable consequences of Private
8 Information ending up in the possession of criminals, the risk of identity theft to
9 the Plaintiff and Class Members has materialized and is imminent, and Plaintiff
10 and Class Members have all sustained actual injuries and damages, including: (i)
11 invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished
12 value of Private Information; (iv) lost time and opportunity costs associated with
13 attempting to mitigate the actual consequences of the Data Breach; (v) lost
14 opportunity costs associated with attempting to mitigate the actual consequences
15 of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) the
16 continued and certainly increased risk to their Private Information, which: (a)
17 remains unencrypted and available for unauthorized third parties to access and
18 abuse; and (b) remains backed up in Defendant's possession and is subject to
19 further unauthorized disclosures so long as Defendant fails to undertake
20 appropriate and adequate measures to protect the Private Information.
21
22
23
24
25
26

27 ***The Data Breach Increases Plaintiff's and Class Member's Risk of*** 28 ***Identity Theft***

1
2 103. Plaintiff and Class Members are at a present and continued risk of
3 identity theft for years to come.

4 104. As Plaintiff has already experienced, the unencrypted Private
5 Information of Class Members has or will be available for sale on the dark web
6 because that is the *modus operandi* of hackers.

7
8 105. In addition, unencrypted Private Information may fall into the hands
9 of companies that will use the detailed Private Information for targeted marketing
10 without the approval of Plaintiff and Class Members.
11

12 106. Unauthorized individuals can easily access the Private Information
13 of Plaintiff and Class Members.
14

15 107. The link between a data breach and the risk of identity theft is simple
16 and well established. Criminals acquire and steal Private Information to monetize
17 the information. Criminals monetize the data by selling the stolen information on
18 the black market to other criminals who then utilize the information to commit a
19 variety of identity theft related crimes discussed below.
20
21

22 108. Because a person's identity is akin to a puzzle with multiple data
23 points, the more accurate pieces of data an identity thief obtains about a person,
24 the easier it is for the thief to take on the victim's identity--or track the victim to
25 attempt other hacking crimes against the individual to obtain more data to perfect
26 a crime.
27
28

1 109. For example, armed with just a name and date of birth, a data thief
2 can utilize a hacking technique referred to as “social engineering” to obtain even
3 more information about a victim’s identity, such as a person’s login credentials
4 or Social Security number. Social engineering is a form of hacking whereby a
5 data thief uses previously acquired information to manipulate and trick
6 individuals into disclosing additional confidential or personal information
7 through means such as spam phone calls and text messages or phishing emails.
8 Data Breaches can be the starting point for these additional targeted attacks on
9 the victims.
10
11

12
13 110. One such example of criminals piecing together bits and pieces of
14 compromised Private Information for profit is the development of “Fullz”
15 packages.³³
16
17
18

19 ³³ “Fullz” is fraudster speak for data that includes the information of the victim, including, but not
20 limited to, the name, address, credit card information, social security number, date of birth, and
21 more. As a rule of thumb, the more information you have on a victim, the more money that can be
22 made off of those credentials. Fullz are usually pricier than standard credit card credentials,
23 commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning
24 credentials into money) in various ways, including performing bank transactions over the phone
25 with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials
26 associated with credit cards that are no longer valid, can still be used for numerous purposes,
27 including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule
28 account” (an account that will accept a fraudulent money transfer from a compromised account)
without the victim’s knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground*
Stolen From Texas Life Insurance Firm, Krebs on Security (Sep. 18, 2014),
[https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-)
[texas-life-insurance-\]\(https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/)
[underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/)

1 111. With “Fullz” packages, cyber-criminals can cross-reference two
2 sources of Private Information to marry unregulated data available elsewhere to
3 criminally stolen data with an astonishingly complete scope and degree of
4 accuracy in order to assemble complete dossiers on individuals.
5

6 112. The development of “Fullz” packages means here that the stolen
7 Private Information from the Data Breach can easily be used to link and identify
8 it to Plaintiff’s and Class Members’ phone numbers, email addresses, and other
9 unregulated sources and identifiers. In other words, even if certain information
10 such as emails, phone numbers, or credit card numbers may not be included in
11 the Private Information that was exfiltrated in the Data Breach, criminals may
12 still easily create a Fullz package and sell it at a higher price to unscrupulous
13 operators and criminals (such as illegal and scam telemarketers) over and over.
14
15

16 113. The existence and prevalence of “Fullz” packages means that the
17 Private Information stolen from the data breach can easily be linked to the
18 unregulated data (like driver's license numbers) of Plaintiff and the other Class
19 Members.
20
21

22 114. Thus, even if certain information (such as driver's license numbers)
23 was not stolen in the data breach, criminals can still easily create a comprehensive
24 “Fullz” package.
25
26
27
28

1 115. Then, this comprehensive dossier can be sold—and then resold in
2 perpetuity—to crooked operators and other criminals (like illegal and scam
3 telemarketers).
4

5 ***Loss of Time to Mitigate the Risk of Identity Theft and Fraud***

6 116. As a result of the recognized risk of identity theft, when a Data
7 Breach occurs, and an individual is notified by a company that their Private
8 Information was compromised, as in this Data Breach, the reasonable person is
9 expected to take steps and spend time to address the dangerous situation, learn
10 about the breach, and otherwise mitigate the risk of becoming a victim of identity
11 theft of fraud. Failure to spend time taking steps to review accounts or credit
12 reports could expose the individual to greater financial harm – yet, the resource
13 and asset of time has been lost.
14
15
16

17 117. Thus, due to the actual and imminent risk of identity theft that
18 Plaintiff and Class Members face, Defendant’s Notice Letter instructs Plaintiff
19 and Class Members to do the following: “[w]e encourage you to remain vigilant
20 and regularly review your account statements and credit report for any incidents
21 of fraud, identity theft, or unauthorized activity.”³⁴
22
23

24 118. Plaintiff and Class Members have spent, and will spend additional
25 time in the future, on a variety of prudent actions, such as researching and
26

27 ³⁴ Notice Letter.
28

1 verifying the legitimacy of the Data Breach and contacting Defendant to obtain
2 more information about the Data Breach's occurrence.

3
4 119. Plaintiff's mitigation efforts are consistent with the U.S. Government
5 Accountability Office that released a report in 2007 regarding data breaches
6 ("GAO Report") in which it noted that victims of identity theft will face
7 "substantial costs and time to repair the damage to their good name and credit
8 record."³⁵

9
10 120. Plaintiff's mitigation efforts are also consistent with the steps that
11 FTC recommends that data breach victims take several steps to protect their
12 personal and financial information after a data breach, including: contacting one
13 of the credit bureaus to place a fraud alert (consider an extended fraud alert that
14 lasts for seven years if someone steals their identity), reviewing their credit
15 reports, contacting companies to remove fraudulent charges from their accounts,
16 placing a credit freeze on their credit, and correcting their credit reports.³⁶

17
18
19 121. And for those Class Members who experience actual identity theft
20 and fraud, the United States Government Accountability Office released a report
21 in 2007 regarding data breaches ("GAO Report") in which it noted that victims
22
23
24

25 ³⁵ See United States Government Accountability Office, GAO-07-737, Personal Information: Data
26 Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full
27 Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

28 ³⁶ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps>

1 of identity theft will face “substantial costs and time to repair the damage to their
2 good name and credit record.”³⁷

3
4 ***Diminution Value of Private Information***

5 122. PII and PHI are valuable property rights.³⁸ Their value is axiomatic,
6 considering the value of Big Data in corporate America and the consequences of
7 cyber thefts include heavy prison sentences. Even this obvious risk to reward
8 analysis illustrates beyond doubt that Private Information has considerable
9 market value.
10

11 123. For example, drug manufacturers, medical device manufacturers,
12 pharmacies, hospitals and other entities in custody of PII often purchase PII on
13 the black market for the purpose of target marketing their products and services
14 to the physical maladies of the data breach victims himself. Insurance companies
15 purchase and use wrongfully disclosed Private Information to adjust their
16 insureds’ medical insurance premiums.
17
18
19
20
21
22

23 ³⁷ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited;
24 However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007,
<https://www.gao.gov/new.items/d07737.pdf> (“GAO Report”).

25 ³⁸ See, e.g., John T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable
26 Information (“Private Information”) Equals the “Value” of Financial Assets, 15 Rich. J.L. & Tech.
27 11, at *3-4 (2009) (“Private Information, which companies obtain at little cost, has quantifiable
28 value that is rapidly reaching a level comparable to the value of traditional financial assets.”)
(citations omitted).

124. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly \$200 billion.³⁹ In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{40,41}

125. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.⁴²

126. Sensitive PII can sell for as much as \$363 per record according to the Infosec Institute.⁴³

127. Theft of PHI is also gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”⁴⁴

³⁹ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

⁴⁰ <https://datacoup.com/>

⁴¹ <https://digi.me/what-is-digime/>

⁴² Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqen.html>

⁴³ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>

⁴⁴ *Medical I.D. Theft, EFraudPrevention* <https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected.> (last visited Nov. 6, 2023).

1 128. As a result of the Data Breach, Plaintiff's and Class Members'
2 Private Information, which has an inherent market value in both legitimate and
3 dark markets, has been damaged and diminished by its compromise and
4 unauthorized release. However, this transfer of value occurred without any
5 consideration paid to Plaintiff or Class Members for their property, resulting in
6 an economic loss. Moreover, the Private Information is now readily available, and
7 the rarity of the Data has been lost, thereby causing additional loss of value.
8

9
10 129. Based on the foregoing, the information compromised in the Data
11 Breach is significantly more valuable than the loss of, for example, credit card
12 information in a retailer data breach because, there, victims can cancel or close
13 credit and debit card accounts. The information compromised in this Data Breach
14 is impossible to "close" and difficult, if not impossible, to change, e.g., Social
15 Security numbers, PHI, dates of birth, and names.
16

17
18 130. Among other forms of fraud, identity thieves may obtain driver's
19 licenses, government benefits, medical services, and housing or even give false
20 information to police.
21

22 131. The fraudulent activity resulting from the Data Breach may not come
23 to light for years.
24

25 132. At all relevant times, Defendant knew, or reasonably should have
26 known, of the importance of safeguarding the Private Information of Plaintiff and
27
28

1 Class Members, and of the foreseeable consequences that would occur if
2 Defendant's data security system was breached, including, specifically, the
3 significant costs that would be imposed on Plaintiff and Class Members as a result
4 of a breach.
5

6 133. Plaintiff and Class Members now face years of constant surveillance
7 of their financial and personal records, monitoring, and loss of rights. The Class
8 is incurring and will continue to incur such damages in addition to any fraudulent
9 use of their Private Information.
10

11 134. Defendant was, or should have been, fully aware of the unique type
12 and the significant volume of data on Defendant's network, amounting to, upon
13 information and belief, thousands to tens of thousands of individuals' detailed
14 personal information and, thus, the significant number of individuals who would
15 be harmed by the exposure of the unencrypted data.
16

17 135. The injuries to Plaintiff and Class Members were directly and
18 proximately caused by Defendant's failure to implement or maintain adequate
19 data security measures for the Private Information of Plaintiff and Class
20 Members.
21

22 ***Future Costs of Credit and Identity Theft Monitoring is Reasonable and***
23 ***Necessary***
24

25 136. Given the type of targeted attack in this case and sophisticated
26 criminal activity, the type of Private Information involved, the volume of Private
27
28

1 Information accessed in the Data Breach, and Plaintiff's Private Information
2 already being disseminated on the dark web (as discussed below), there is a strong
3 probability that entire batches of stolen information have been placed, or will be
4 placed, on the black market/dark web for sale and purchase by criminals intending
5 to utilize the Private Information for identity theft crimes –e.g., opening bank
6 accounts in the victims' names to make purchases or to launder money; file false
7 tax returns; take out loans or lines of credit; or file false unemployment claims.
8

9
10 137. Such fraud may go undetected until debt collection calls commence
11 months, or even years, later.
12

13 138. An individual may not know that his or her Social Security Number
14 was used to file for unemployment benefits until law enforcement notifies the
15 individual's employer of the suspected fraud. Fraudulent tax returns are typically
16 discovered only when an individual's authentic tax return is rejected.
17

18 139. Furthermore, the information accessed and disseminated in the Data
19 Breach is significantly more valuable than the loss of, for example, credit card
20 information in a retailer data breach, where victims can easily cancel or close
21 credit and debit card accounts.⁴⁵ The information disclosed in this Data Breach is
22
23
24
25

26 ⁴⁵ See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web, New Report Finds*,
27 FORBES (Mar. 25, 2020), <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1>.
28

1 impossible to “close” and difficult, if not impossible, to change (such as Social
2 Security numbers).

3
4 140. Consequently, Plaintiff and Class Members are at a present and
5 continuous risk of fraud and identity theft for many years into the future.

6 141. The retail cost of credit monitoring and identity theft monitoring can
7 cost around \$200 a year per Class Member. This is reasonable and necessary cost
8 to monitor to protect Class Members from the risk of identity theft that arose from
9 Defendant’s Data Breach.
10

11
12 ***Plaintiff Joseph Biondi’s Experience***

13 142. Plaintiff Biondi was not familiar with Defendant prior to receiving the
14 Notice Letter in the mail, but, upon information and belief, Defendant obtained his
15 Private Information in the course of its regular business operations.
16

17 143. Plaintiff Biondi is very careful about sharing his sensitive Private
18 Information. Plaintiff stores any documents containing his Private Information in
19 a safe and secure location. He has never knowingly transmitted unencrypted
20 sensitive Private Information over the internet or any other unsecured source.
21

22 144. At the time of the Data Breach—approximately December 1, 2022
23 through January 2, 2023—Defendant retained Plaintiff’s Private Information in
24 its system.
25

26 145. Plaintiff Biondi received the Notice Letter, by email, directly from
27
28

1 Defendant, dated February 8, 2024. According to the Notice Letter, Plaintiff's
2 Private Information was improperly accessed and obtained by unauthorized third
3 parties, including his full name, date of birth, driver's license number or state
4 identification number, financial account number, financial account access
5 information, health insurance identification number, information related to
6 medical treatment or diagnosis, passport number, payment card number, payment
7 card access information, Social Security Number, and/or username and password.
8

9
10 146. As a result of the Data Breach, and at the direction of Defendant's
11 Notice Letter, which instructs Plaintiff to "remain vigilant and regularly review
12 your account statements and credit report for any incidents of fraud, identity theft,
13 or unauthorized activity[.]"⁴⁶ Plaintiff made reasonable efforts to mitigate the
14 impact of the Data Breach, including but not limited to: researching and verifying
15 the legitimacy of the Data Breach and contacting Defendant to obtain more
16 information about the Data Breach's occurrence. Plaintiff have spent significant
17 on mitigation activities in response to the Data Breach—valuable time Plaintiff
18 otherwise would have spent on other activities, including but not limited to work
19 and/or recreation. This time has been lost forever and cannot be recaptured.
20
21
22
23

24 147. Subsequent to the Data Breach, Plaintiff Biondi has suffered
25 numerous, substantial injuries including, but not limited to: (i) invasion of
26

27 ⁴⁶ Notice Letter.
28

1 privacy; (ii) theft of his Private Information; (iii) lost or diminished value of
2 Private Information; (iv) lost time and opportunity costs associated with
3 attempting to mitigate the actual consequences of the Data Breach; (v) lost
4 opportunity costs associated with attempting to mitigate the actual consequences
5 of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) the
6 continued and certainly increased risk to his Private Information, which: (a)
7 remains unencrypted and available for unauthorized third parties to access and
8 abuse; and (b) remains backed up in Defendant's possession and is subject to
9 further unauthorized disclosures so long as Defendant fails to undertake
10 appropriate and adequate measures to protect the Private Information.
11
12
13

14 148. Plaintiff additionally suffered actual injury in the form of his Private
15 Information being disseminated on the dark web, according to Experian, which,
16 upon information and belief, was caused by the Data Breach.
17
18

19 149. Plaintiff further suffered actual injury in the form of experiencing an
20 increase in spam calls, texts, and/or emails, which, upon information and belief,
21 was caused by the Data Breach.
22

23 150. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress,
24 which has been compounded by the fact that Defendant has still not fully informed
25 him of key details about the Data Breach's occurrence.
26
27
28

1 151. As a result of the Data Breach, Plaintiff anticipates spending
2 considerable time and money on an ongoing basis to try to mitigate and address
3 harms caused by the Data Breach.
4

5 152. As a result of the Data Breach, Plaintiff is at a present risk and will
6 continue to be at increased risk of identity theft and fraud for years to come.
7

8 153. Plaintiff Biondi has a continuing interest in ensuring that his Private
9 Information, which, upon information and belief, remains backed up in Defendant's
10 possession, is protected and safeguarded from future breaches.
11

12 **CLASS ACTION ALLEGATIONS**

13 154. Plaintiff brings this action on behalf of himself and on behalf of all other
14 persons similarly situated.
15

16 155. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff proposes the
17 following Class definition, subject to amendment as appropriate:
18

19 **Nationwide Class**

20 All individuals in the United States whose Private Information was impacted
21 as a result of the Data Breach announced by Defendant in February 2024 (the
22 "Class").

23 156. Excluded from the Class are Defendant's officers and directors, and any
24 entity in which Defendant has a controlling interest; and the affiliates, legal
25 representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded
26 also from the Class are members of the judiciary to whom this case is assigned, their
27 families and members of their staff.
28

1 157. Plaintiff hereby reserves the right to amend or modify the Class
2 definition with greater specificity or division after having had an opportunity to
3 conduct discovery.
4

5 158. Numerosity. The Members of the Class are so numerous that joinder of
6 all of them is impracticable. While the exact number of Class Members is unknown
7 to Plaintiff at this time and exclusively in the possession of Defendant, upon
8 information and belief, thousands of individuals were impacted in the Data Breach.
9

10 159. Commonality. There are questions of law and fact common to the Class,
11 which predominate over any questions affecting only individual Class Members.
12 These common questions of law and fact include, without limitation:
13

- 14 a. Whether Defendant unlawfully used, maintained, lost, or disclosed
15 Plaintiff's and Class Members' Private Information;
16
- 17 b. Whether Defendant failed to implement and maintain reasonable
18 security procedures and practices appropriate to the nature and scope
19 of the information compromised in the Data Breach;
20
- 21 c. Whether Defendant's data security systems prior to and during the
22 Data Breach complied with applicable data security laws and
23 regulations;
24
- 25 d. Whether Defendant's data security systems prior to and during the
26 Data Breach were consistent with industry standards;
27
28

- e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;
- f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;
- g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;
- h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- j. Whether Defendant's conduct was negligent;
- k. Whether Defendant breached implied contracts for adequate data security with Plaintiff and Class Members;
- l. Whether Defendant was unjustly enriched by retention of the monetary benefits conferred on it by Plaintiff and Class Members;
- m. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and,
- n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

1 160. Typicality. Plaintiff's claims are typical of those of other Class
2 Members because Plaintiff's Private Information, like that of every other Class
3 Member, was compromised in the Data Breach.
4

5 161. Adequacy of Representation. Plaintiff will fairly and adequately
6 represent and protect the interests of the Members of the Class. Plaintiff's Counsel
7 are competent and experienced in litigating class actions.
8

9 162. Predominance. Defendant has engaged in a common course of conduct
10 toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members'
11 Private Information was stored on the same computer systems and unlawfully
12 accessed in the same way. The common issues arising from Defendant's conduct
13 affecting Class Members set out above predominate over any individualized issues.
14 Adjudication of these common issues in a single action has important and desirable
15 advantages of judicial economy.
16
17

18 163. Superiority. A class action is superior to other available methods for the
19 fair and efficient adjudication of the controversy. Class treatment of common
20 questions of law and fact is superior to multiple individual actions or piecemeal
21 litigation. Absent a class action, most Class Members would likely find that the cost
22 of litigating their individual claims is prohibitively high and would therefore have
23 no effective remedy. The prosecution of separate actions by individual Class
24 Members would create a risk of inconsistent or varying adjudications with respect
25
26
27
28

1 to individual Class Members, which would establish incompatible standards of
2 conduct for Defendant. In contrast, the conduct of this action as a class action
3 presents far fewer management difficulties, conserves judicial resources and the
4 parties' resources, and protects the rights of each Class Member.
5

6 164. Defendant has acted on grounds that apply generally to the Class as a
7 whole, so that class certification, injunctive relief, and corresponding declaratory
8 relief are appropriate on a class-wide basis.
9

10 165. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are
11 appropriate for certification because such claims present only particular, common
12 issues, the resolution of which would advance the disposition of this matter and the
13 parties' interests therein. Such particular issues include, but are not limited to:
14

- 15 a. Whether Defendant owed a legal duty to Plaintiff and the Class to
16 exercise due care in collecting, storing, and safeguarding their
17 Private Information;
18
- 19 b. Whether Defendant's security measures to protect its data systems
20 were reasonable in light of best practices recommended by data
21 security experts;
22
- 23 c. Whether Defendant's failure to institute adequate protective security
24 measures amounted to negligence;
25
26
27
28

1 d. Whether Defendant failed to take commercially reasonable steps to
2 safeguard consumer Private Information; and

3 e. Whether adherence to FTC data security recommendations, and
4 measures recommended by data security experts would have
5 reasonably prevented the Data Breach.
6

7
8 166. Finally, all Members of the proposed Class are readily ascertainable.
9 Defendant has access to Class Members' names and addresses affected by the Data
10 Breach. Class Members have already been preliminarily identified and sent Notice
11 of the Data Breach by Defendant.
12

13 **COUNT I**
14 **Negligence**
15 **(On behalf of Plaintiff and the Class)**

16 167. Plaintiff re-alleges and incorporates the above allegations as if fully
17 set forth herein.

18 168. Defendant requires its employees and employee beneficiaries,
19 including Class Members, to submit non-public Private Information in the
20 ordinary course of providing its services.
21

22 169. Defendant gathered and stored the Private Information of Plaintiff
23 and Class Members as part of its business of soliciting its employees, which
24 solicitations and services affect commerce.
25
26
27
28

1 170. Plaintiff and Class Members entrusted Defendant with their Private
2 Information with the understanding that Defendant would safeguard their
3 information.
4

5 171. Defendant had full knowledge of the sensitivity of the Private
6 Information and the types of harm that Plaintiff and Class Members could and
7 would suffer if the Private Information were wrongfully disclosed.
8

9 172. By assuming the responsibility to collect and store this data, and in
10 fact doing so, and sharing it and using it for commercial gain, Defendant had a
11 duty of care to use reasonable means to secure and to prevent disclosure of the
12 information, and to safeguard the information from theft.
13

14 173. Defendant had a duty to employ reasonable security measures under
15 Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits
16 “unfair . . . practices in or affecting commerce,” including, as interpreted and
17 enforced by the FTC, the unfair practice of failing to use reasonable measures to
18 protect confidential data.
19
20

21 174. Defendant owed a duty of care to Plaintiff and Class Members to
22 provide data security consistent with industry standards and other requirements
23 discussed herein, and to ensure that its systems and networks, and the personnel
24 responsible for them, adequately protected the Private Information.
25
26
27
28

1 175. Defendant's duty of care to use reasonable security measures arose
2 as a result of the special relationship that existed between Defendant and Plaintiff
3 and Class Members. That special relationship arose because Plaintiff and the
4 Class entrusted Defendant with their confidential Private Information, a necessary
5 part of obtaining employment and/or employee benefits at Defendant.
6

7
8 176. Defendant's duty to use reasonable care in protecting confidential
9 data arose not only as a result of the statutes and regulations described above, but
10 also because Defendant is bound by industry standards to protect confidential
11 Private Information.
12

13 177. Defendant was subject to an "independent duty," untethered to any
14 contract between Defendant and Plaintiff or the Class.
15

16 178. Defendant also had a duty to exercise appropriate clearinghouse
17 practices to remove former employees' and employee beneficiaries' Private
18 Information it was no longer required to retain pursuant to regulations.
19

20 179. Moreover, Defendant had a duty to promptly and adequately notify
21 Plaintiff and the Class of the Data Breach.
22

23 180. Defendant had and continues to have a duty to adequately disclose
24 that the Private Information of Plaintiff and the Class within Defendant's
25 possession might have been compromised, how it was compromised, and
26 precisely the types of data that were compromised and when. Such notice was
27
28

1 necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and
2 repair any identity theft and the fraudulent use of their Private Information by
3 third parties.
4

5 181. Defendant breached its duties, pursuant to the FTC Act and other
6 applicable standards, and thus was negligent, by failing to use reasonable
7 measures to protect Class Members' Private Information. The specific negligent
8 acts and omissions committed by Defendant include, but are not limited to, the
9 following:
10

- 11 a. Failing to adopt, implement, and maintain adequate security
12 measures to safeguard Class Members' Private Information;
13
- 14 b. Failing to adequately monitor the security of their networks and
15 systems;
16
- 17 c. Allowing unauthorized access to Class Members' Private
18 Information;
19
- 20 d. Failing to detect in a timely manner that Class Members' Private
21 Information had been compromised;
22
- 23 e. Failing to remove former employees' and employee beneficiaries'
24 Private Information it was no longer required to retain pursuant to
25 regulations,
26
27
28

1 f. Failing to timely and adequately notify Class Members about the
2 Data Breach's occurrence and scope, so that they could take
3 appropriate steps to mitigate the potential for identity theft and other
4 damages; and
5

6 g. Failing to secure its stand-alone personal computers, such as the
7 reception desk computers, even after discovery of the data breach.
8

9 182. Defendant violated Section 5 of the FTC Act by failing to use
10 reasonable measures to protect Private Information and not complying with
11 applicable industry standards, as described in detail herein. Defendant's conduct
12 was particularly unreasonable given the nature and amount of Private Information
13 it obtained and stored and the foreseeable consequences of the immense damages
14 that would result to Plaintiff and the Class.
15
16

17 183. Defendant's violation of Section 5 of the FTC Act constitutes
18 negligence.
19

20 184. Plaintiff and Class Members were within the class of persons the
21 Federal Trade Commission Act was intended to protect and the type of harm that
22 resulted from the Data Breach was the type of harm the statute was intended to
23 guard against.
24

25 185. The FTC has pursued enforcement actions against businesses, which,
26 as a result of their failure to employ reasonable data security measures and avoid
27
28

1 unfair and deceptive practices, caused the same harm as that suffered by Plaintiff
2 and the Class.

3
4 186. A breach of security, unauthorized access, and resulting injury to
5 Plaintiff and the Class was reasonably foreseeable, particularly in light of
6 Defendant's inadequate security practices.

7
8 187. It was foreseeable that Defendant's failure to use reasonable
9 measures to protect Class Members' Private Information would result in injury to
10 Class Members. Further, the breach of security was reasonably foreseeable given
11 the known high frequency of cyberattacks and data breaches targeting employers
12 in possession of Private Information.

13
14 188. Defendant has full knowledge of the sensitivity of the Private
15 Information and the types of harm that Plaintiff and the Class could and would
16 suffer if the Private Information were wrongfully disclosed.

17
18 189. Plaintiff and the Class were the foreseeable and probable victims of
19 any inadequate security practices and procedures. Defendant knew or should have
20 known of the inherent risks in collecting and storing the Private Information of
21 Plaintiff and the Class, the critical importance of providing adequate security of
22 that Private Information, and the necessity for encrypting Private Information
23 stored on Defendant's systems.
24
25
26
27
28

1 190. It was therefore foreseeable that the failure to adequately safeguard
2 Class Members' Private Information would result in one or more types of injuries
3 to Class Members.
4

5 191. Plaintiff and the Class had no ability to protect their Private
6 Information that was in, and possibly remains in, Defendant's possession.
7

8 192. Defendant was in a position to protect against the harm suffered by
9 Plaintiff and the Class as a result of the Data Breach.
10

11 193. Defendant's duty extended to protecting Plaintiff and the Class from
12 the risk of foreseeable criminal conduct of third parties, which has been
13 recognized in situations where the actor's own conduct or misconduct exposes
14 another to the risk or defeats protections put in place to guard against the risk, or
15 where the parties are in a special relationship. *See* Restatement (Second) of Torts
16 § 302B. Numerous courts and legislatures have also recognized the existence of
17 a specific duty to reasonably safeguard personal information.
18
19

20 194. Defendant has admitted that the Private Information of Plaintiff and
21 the Class was wrongfully lost and disclosed to unauthorized third persons as a
22 result of the Data Breach.
23

24 195. But for Defendant's wrongful and negligent breach of duties owed to
25 Plaintiff and the Class, the Private Information of Plaintiff and the Class would
26 not have been compromised.
27
28

1 196. There is a close causal connection between Defendant's failure to
2 implement security measures to protect the Private Information of Plaintiff and
3 the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the
4 Class. The Private Information of Plaintiff and the Class was lost and accessed as
5 the proximate result of Defendant's failure to exercise reasonable care in
6 safeguarding such Private Information by adopting, implementing, and
7 maintaining appropriate security measures.

10 197. As a direct and proximate result of Defendant's negligence, Plaintiff
11 and the Class have suffered and will suffer injury, including but not limited to: (i)
12 invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished
13 value of Private Information; (iv) lost time and opportunity costs associated with
14 attempting to mitigate the actual consequences of the Data Breach; (v) lost
15 opportunity costs associated with attempting to mitigate the actual consequences of
16 the Data Breach; (vi) experiencing an increase in spam calls, texts, and/or emails;
17 (vii) Plaintiff's Private Information being disseminated on the dark web, according
18 to Experian; (viii) statutory damages; (ix) nominal damages; and (x) the continued
19 and certainly increased risk to their Private Information, which: (a) remains
20 unencrypted and available for unauthorized third parties to access and abuse; and (b)
21 remains backed up in Defendant's possession and is subject to further unauthorized
22
23
24
25
26
27
28

1 disclosures so long as Defendant fails to undertake appropriate and adequate
2 measures to protect the Private Information.

3
4 198. As a direct and proximate result of Defendant's negligence, Plaintiff
5 and the Class have suffered and will continue to suffer other forms of injury
6 and/or harm, including, but not limited to, anxiety, emotional distress, loss of
7 privacy, and other economic and non-economic losses.
8

9 199. Additionally, as a direct and proximate result of Defendant's
10 negligence, Plaintiff and the Class have suffered and will suffer the continued
11 risks of exposure of their Private Information, which remain in Defendant's
12 possession and is subject to further unauthorized disclosures so long as Defendant
13 fails to undertake appropriate and adequate measures to protect the Private
14 Information in its continued possession.
15
16

17 200. Plaintiff and Class Members are entitled to compensatory and
18 consequential damages suffered as a result of the Data Breach.
19

20 201. Defendant's negligent conduct is ongoing, in that it still holds the
21 Private Information of Plaintiff and Class Members in an unsafe and insecure
22 manner.
23

24 202. Plaintiff and Class Members are also entitled to injunctive relief
25 requiring Defendant to (i) strengthen its data security systems and monitoring
26 procedures; (ii) submit to future annual audits of those systems and monitoring
27
28

1 procedures; and (iii) continue to provide adequate credit monitoring to all Class
2 Members.

3
4 **COUNT II**
5 **Unjust Enrichment**
6 **(On Behalf of Plaintiff and the Class)**

7 203. Plaintiff re-alleges and incorporates the above allegations as if fully
8 set forth herein.

9 204. Plaintiff and Class Members conferred a monetary benefit on
10 Defendant by providing Defendant with their labor and/or their Private
11 Information to Defendant.
12

13 205. Defendant appreciated that a monetary benefit was being conferred
14 upon it by Plaintiff and Class Members and accepted that monetary benefit.
15

16 206. However, acceptance of the benefit under the facts and circumstances
17 outlined above make it inequitable for Defendant to retain that benefit without
18 payment of the value thereof.
19

20 207. Specifically, Defendant enriched itself by saving the costs it
21 reasonably should have expended on data security measures to secure Plaintiff's
22 and Class Members' Personal Information. Instead of providing a reasonable
23 level of security that would have prevented the Data Breach, Defendant instead
24 calculated to increase its own profits at the expense of Plaintiff and Class
25 Members by utilizing cheaper, ineffective security measures. Plaintiff and Class
26
27
28

1 Members, on the other hand, suffered as a direct and proximate result of
2 Defendant's decision to prioritize its own profits over the requisite data security.
3

4 208. Under the principles of equity and good conscience, Defendant
5 should not be permitted to retain the monetary benefit belonging to Plaintiff and
6 Class Members, because Defendant failed to implement appropriate data
7 management and security measures.
8

9 209. Defendant acquired the Private Information through inequitable
10 means in that it failed to disclose the inadequate security practices previously
11 alleged.
12

13 210. If Plaintiff and Class Members knew that Defendant had not secured
14 their Private Information, they would not have agreed to provide their Private
15 Information to Defendant or obtained employment and/or employee benefits at
16 Defendant.
17

18 211. Plaintiff and Class Members have no adequate remedy at law.
19

20 212. As a direct and proximate result of Defendant's conduct, Plaintiff and
21 Class Members have suffered or will suffer injury, including but not limited to: (i)
22 invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished
23 value of Private Information; (iv) lost time and opportunity costs associated with
24 attempting to mitigate the actual consequences of the Data Breach; (v) lost
25 opportunity costs associated with attempting to mitigate the actual consequences of
26
27
28

1 the Data Breach; (vi) experiencing an increase in spam calls, texts, and/or emails;
2 (vii) Plaintiff's Private Information being disseminated on the dark web, according
3 to Experian; (viii) statutory damages; (ix) nominal damages; and (x) the continued
4 and certainly increased risk to their Private Information, which: (a) remains
5 unencrypted and available for unauthorized third parties to access and abuse; and (b)
6 remains backed up in Defendant's possession and is subject to further unauthorized
7 disclosures so long as Defendant fails to undertake appropriate and adequate
8 measures to protect the Private Information.
9
10

11
12 213. As a direct and proximate result of Defendant's conduct, Plaintiff and
13 Class Members have suffered and will continue to suffer other forms of injury
14 and/or harm.
15

16 214. Defendant should be compelled to disgorge into a common fund or
17 constructive trust, for the benefit of Plaintiff and Class Members, proceeds that
18 they unjustly received from them.
19

20 **PRAYER FOR RELIEF**

21 **WHEREFORE**, Plaintiff, on behalf of himself and Class Members, requests
22 judgment against Defendant and that the Court grants the following:
23

24 A. For an Order certifying this action as a class action and appointing
25 Plaintiff and his counsel to represent the Class;
26
27
28

1 B. For equitable relief enjoining Defendant from engaging in the wrongful
2 conduct complained of herein pertaining to the misuse and/or
3 disclosure of Plaintiff's and Class Members' Private Information, and
4 from refusing to issue prompt, complete and accurate disclosures to
5 Plaintiff and Class Members;
6

7
8 C. For injunctive relief requested by Plaintiff, including, but not limited
9 to, injunctive and other equitable relief as is necessary to protect the
10 interests of Plaintiff and Class Members, including but not limited to
11 an order:
12

13 i. prohibiting Defendant from engaging in the wrongful and
14 unlawful acts described herein;
15

16 ii. requiring Defendant to protect, including through
17 encryption, all data collected through the course of their
18 business in accordance with all applicable regulations,
19 industry standards, and federal, state or local laws;
20

21 iii. requiring Defendant to delete, destroy, and purge the personal
22 identifying information of Plaintiff and Class Members unless
23 Defendant can provide to the Court reasonable justification
24 for the retention and use of such information when weighed
25 against the privacy interests of Plaintiff and Class Members;
26
27
28

- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;
- v. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;
- vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things,

1 creating firewalls and access controls so that if one area of
2 Defendant's network is compromised, hackers cannot gain
3 access to other portions of Defendant's systems;
4

5 ix. requiring Defendant to conduct regular database scanning and
6 securing checks;
7

8 x. requiring Defendant to establish an information security
9 training program that includes at least annual information
10 security training for all employees, with additional training to
11 be provided as appropriate based upon the employees'
12 respective responsibilities with handling personal identifying
13 information, as well as protecting the personal identifying
14 information of Plaintiff and Class Members;
15
16

17 xi. requiring Defendant to routinely and continually conduct
18 internal training and education, and on an annual basis to
19 inform internal security personnel how to identify and contain
20 a breach when it occurs and what to do in response to a
21 breach;
22
23

24 xii. requiring Defendant to implement a system of tests to assess
25 its respective employees' knowledge of the education
26 programs discussed in the preceding subparagraphs, as well
27
28

1 as randomly and periodically testing employees compliance
2 with Defendant's policies, programs, and systems for
3 protecting personal identifying information;
4

5 xiii. requiring Defendant to implement, maintain, regularly
6 review, and revise as necessary a threat management program
7 designed to appropriately monitor Defendant's information
8 networks for threats, both internal and external, and assess
9 whether monitoring tools are appropriately configured,
10 whether monitoring tools are appropriately configured,
11 tested, and updated;
12

13 xiv. requiring Defendant to meaningfully educate all Class
14 Members about the threats that they face as a result of the loss
15 of their confidential personal identifying information to third
16 parties, as well as the steps affected individuals must take to
17 protect himself;
18

19 xv. requiring Defendant to implement logging and monitoring
20 programs sufficient to track traffic to and from Defendant's
21 servers; and
22

23 xvi. for a period of 10 years, appointing a qualified and
24 independent third party assessor to conduct a SOC 2 Type 2
25 attestation on an annual basis to evaluate Defendant's
26
27
28

1 compliance with the terms of the Court's final judgment, to
2 provide such report to the Court and to counsel for the class,
3 and to report any deficiencies with compliance of the Court's
4 final judgment;
5

6 D. For an award of actual damages, compensatory damages, statutory
7 damages, and nominal damages, in an amount to be determined, as
8 allowable by law;
9

10 E. For an award of punitive damages, as allowable by law;
11

12 F. For an award of attorneys' fees and costs, and any other expense,
13 including expert witness fees;
14

15 G. Pre- and post-judgment interest on any amounts awarded; and
16

17 H. Such other and further relief as this court may deem just and proper.
18

19 **DEMAND FOR JURY TRIAL**

20 Plaintiff hereby demands that this matter be tried before a jury.

21 Dated: February 27, 2024

22 Respectfully submitted,

23 /s/ John J. Nelson

24 John J. Nelson (SBN 317598)

25 **MILBERG COLEMAN BRYSON**

26 **PHILLIPS GROSSMAN, PLLC**

27 280 S. Beverly Drive

28 Beverly Hills, CA 90212

Tel.: (858) 209-6941

jnelson@milberg.com

Counsel for Plaintiff and the Proposed Class